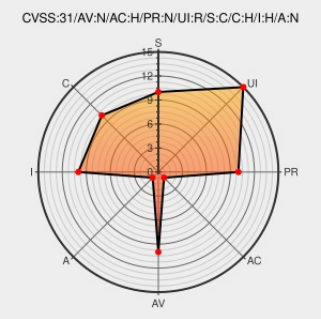
CVE-2020-15134

Published on: 07/31/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:41 PM UTC

CVE-2020-15134 - advisory for GHSA-3q49-h8f9-9fr9

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Faye from Faye Project contain the following vulnerability:

Faye before version 1.4.0, there is a lack of certification validation in TLS handshakes. Faye uses em-http-request and faye-websocket in the Ruby version of its client. Those libraries both use the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for the expected hostname. That means that any `https:` or `wss:` connection made using these libraries is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. The first request a Faye client makes is always sent via normal HTTP, but later messages may be sent via WebSocket. Therefore it is vulnerable to the same problem that these underlying libraries are, and we needed both libraries to support TLS verification before Faye could claim to do the same. Your client would still be insecure if its initial HTTPS request was verified, but later WebSocket connections were not. This is fixed in Faye v1.4.0, which enables verification by default. For further background information on this issue, please see the referenced GitHub Advisory.

CVE-2020-15134 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **faye** - **faye** version **< 1.4.0**

CVSS3 Score: 8.7 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	HIGH	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	NONE

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
Missing TLS certificate verification · Advisory · faye/faye · GitHub	Exploit, Third Party Advisory, github.com, text/html	CONFIRM github.com/faye/faye/security/advisories/GHSA-3q49-h8f9-9fr9
Missing TLS certificate verification in Faye – The If Works	Exploit, Third Party Advisory, blog.jcoglan.com, text/html	MISC blog.jcoglan.com/2020/07/31/missing-tls-verification-in-faye/

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

180681 Debian Security Update for ruby-faye (CVE-2020-15134)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Faye Project	Faye	All	All	All	All
Application	Faye Project	Faye	All	All	All	All

cpe:2.3:a:faye_project:faye:*:*:*:*:*:*:*:*:

cpe:2.3:a:faye_project:faye:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID Next ID→

site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report